This record is a partial extract of the original cable. The full text of the original cable is not available.

UNCLAS SECTION 01 OF 04 OTTAWA 000334

SIPDIS

SENSITIVE

STATE FOR EB/TPP/BTA EB/ESC/ISC (MCMANUS AND ERVITI),
WHA/CAN (MASON AND RUNNING), OES/EGC (MIOTKE AND
DEROSA), D/HS (OPTICAN) AND PM (MARKOFF)

HOMELAND SECURITY FOR EPR (BROWN)

DOE FOR INT'L AND POLICY (A/S BAILEY) AND IE-141 (DEUTSCH)

DOE PASS FERC FOR KELLY AND LEKANG

DOT FOR OFFICE OF PIPELINE SAFETY

COMMERCE FOR 4320/MAC/WH/ON/OIA/BENDER

PARIS FOR IEA

E.O. 12958: N/A
TAGS: EPET ETRD EINV CA
SUBJECT: CRITICAL INFRASTRUCTURE PROTECTION IN
CANADA'S OIL AND GAS PIPELINE NETWORK

SUMMARY/INTRODUCTION

¶1. (U) This message is sensitive, but unclassified. Please handle accordingly.

¶2. (U) This message was prepared with assistance from Amconsul Calgary.

¶3. (U) Critical infrastructure protection is among the areas listed for bilateral action in the Ridge-Manley Smart Border plan. Canada is the United States' largest foreign supplier of energy, supplying over 15 percent of U.S. natural gas consumption and about 10 percent of U.S. consumption of oil and oil products. After two decades of strong expansion, Canada's energy pipeline industry expects to see on the order of US$6 billion in additional new facilities constructed in the coming decade.

¶4. (U) This industry appears very well prepared to respond to accidents/attacks at its facilities. Time frames for pipeline firms' "patch and repair" operations are from a few hours to a few days. The built-in redundancy of pipeline systems (multiple pipes, storage facilities, interconnects, back-up compressors) mean that actual disruptions of supply (at least beyond the local level or for short periods) are considered unlikely.

¶5. (SBU) While the incidence of accidental events has been reduced to a very low level, pipeline industry security experts are less confident of their ability to anticipate or prevent deliberate attacks. It is in this area that they are most receptive to government support - and most interested in clear, timely information flow. Given their degree of professional competence and accountability, and since they provide information "up" to government whenever asked, they want to share more fully in the flow of information "down" from federal level security agencies. One provincial government security official said it has been a "major achievement" to get the RCMP (federal police) to allow even the unclassified versions of threat assessments to be distributed to selected private sector players. END SUMMARY

INDUSTRY STRUCTURE

¶6. (U) Most of Canada's oil and gas pipeline network originates in the province of Alberta (with fingers into British Columbia, Saskatchewan and the Northwest Territories) and transports products southward and/or eastward to the United States and central/eastern Canada. The industry is collectively represented by the Canadian Energy Pipeline Association (cepa.com), based in Calgary. Mission economic staff interviewed industry and government representatives on critical infrastructure protection issues in Ottawa, Calgary and Edmonton during January 2003.

¶7. (U) The following two firms respectively claim to operate the world's longest natural gas and oil pipeline systems.

TRANSCANADA PIPELINES LIMITED (transcanada.com) operates the largest portion of the natural gas system. From southern Alberta it exports gas to the Pacific Gas Transmission Company, the Montana Power Company, and the Alliance Pipeline (which runs southeast through Iowa and Illinois). Its "Canadian mainline" (actually a group of parallel lines)

carries gas eastward across Saskatchewan and Manitoba to the Winnipeg area, where the line splits into a U.S. portion (continuing across Minnesota, Wisconsin and Michigan) and a Canadian portion (continuing across Ontario to Montreal, Toronto and other urban areas).

ENBRIDGE PIPELINES INC. (enbridge.com) operates key oil and oil products pipelines. Its main crude oil line runs from Edmonton (mid-Alberta) southeastward to Wisconsin, where the line divides to pass both north and south of Lake Michigan. This system serves key oil storage and refinery/petrochemicals complexes in Edmonton, Sarnia (Ontario) and Montreal (Quebec) as well as in the United States.

PAST INCIDENTS WERE ACCIDENTAL

¶8. (U) Emergency planning necessarily makes heavy use of the analysis of past incidents. However, in Canada's pipeline industry, past incidents have been due to material failures - notably stress corrosion cracking (SCC) in pipe walls and disintegration of blades in compressor turbines. The frequency of these problems has been systematically reduced through innovation, inspection and maintenance but they still occur, and there are older facilities in use which may be at higher risk. On the positive side, these older facilities represent part of the built-in redundancy which the system uses to continue service when a failure occurs.

PIPELINE FIRMS LEAD ON-THE-GROUND RESPONSE

¶9. (SBU) Most pipeline facilities are buried, and the force of an explosion/rupture tends to go upward, so damage seldom extends to neighboring pipes. Automatic "block valves" immediately shut off flow through the ruptured segment(s). Neighboring facilities are also shut off until they can be inspected (operating them at very low pressure is also an option).

¶10. (SBU) Pipeline firms say they maintain close relationships with landowners, municipalities, and volunteer fire departments along their routes in order to enhance both monitoring of the pipeline, and emergency response. Company employees help to train local firefighters, and these two groups in combination are the "first responders" to pipeline emergencies.

¶11. (SBU) Typical time to patch a pipeline rupture is one to two days and typical time for restoration of full service is three to four days. Due to system redundancy and storage, service to end users is unlikely to be affected in the meanwhile. If necessary, a "bypass" around a damaged segment can be built in about four days. If a compressor is affected, a temporary replacement can be moved and installed in a day or two, though permanent replacement takes much longer -- one to two years -- due to long delivery times from the manufacturers (GE and Rolls-Royce).

PREVENTION/MITIGATION

¶12. (SBU) While a few politically motivated attacks on oil and gas facilities have occurred, neither of the major pipeline systems has significant experience of being deliberately attacked. Many of their monitoring activities - such as "flying the line" by helicopter at low altitude and "sniffing" for leaks - are oriented toward accidental events. With facilities crossing thousands of miles in very remote areas, corporate security experts admit that there is little they can do to protect all this pipe from deliberate sabotage. Obvious key points (such as compressors, storage facilities, and refineries where an attack could be more disruptive) fortunately are exceptions which can be protected to some degree by conventional security methods.

PROVINCIAL GOVERNMENT ROLE: "SECURITY TEMPLATES"

¶13. (U) The Alberta provincial government requires each of 311 municipalities to identify a full-time employee as Director of Disaster Services. This employee is empowered to declare a state of local emergency, can conscript local resources and labor, and is partially protected from litigation arising from actions taken during a state of emergency.

¶14. (SBU) Alberta's "Critical Infrastructure Protection Plan" is based in part on methods developed by the American Petroleum Institute, and has recently been applied to ten key industries, beginning with oil. Industry and government worked together to classify facilities by level of "criticality." Information such as the list of participants in this process and the list of facilities determined "critical" is not made public. Provincial Disaster Services staff visit each of these facilities, collect contact

information, and make recommendations based on "security templates."

¶15. (SBU) Levels of "alert" (none, low, medium, high, imminent) are also determined from time to time, based on threat assessments received from federal agencies. The "security template" applied to each facility depends on that facility's combination of criticality and threat level, and is based on "best practices." Provincial government officials say that their recommendations represent "minimum expectations" and that operators are driven by insurance concerns to meet or exceed these standards.

FEDERAL GOVERNMENT ROLE: THREAT ASSESSMENTS

¶16. (SBU) Observers and security officials unanimously agree that the GOC's two-year-old Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) is not as far advanced as Alberta Disaster Services in its state of readiness, nor in its close ties to industry. OCIPEP relies on line departments such as Natural Resources Canada (NRCan) to liaise with industry. Mission will examine OCIPEP's broader role and functions in coming months.

¶17. (SBU) From the perspective of industry and local/provincial security officials, the GOC's crucial role is as the source (or at least the conduit) for intelligence information on which "declarations of alert" must be based. Apart from OCIPEP, key agencies here are the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP - Canada's federal police service). Our contacts expressed various uncertainties and dissatisfactions surrounding such intelligence. For example:

-- What intelligence do RCMP and CSIS want from the private sector and the public? One industry leader complained, "We give the police lots of information and they tell us nothing." Potential suppliers of information need to know whether or not what they provided in the past was considered useful. (COMMENT: While our contacts were careful not to criticize the GOC, we sensed that they would like to be reassured about the effectiveness of federal agencies, i.e. whether information reaches analysts and is duly incorporated into threat assessments, and whether different parts of the GOC are sharing information with each other. END COMMENT).

-- How much detail will be disseminated? Currently, RCMP and CSIS prepare both classified and unclassified versions of threat assessments; only the latter is shared with provincial governments and industry representatives. Also, in their support of intelligence gathering, firms provide RCMP and CSIS with commercially sensitive information from time to time, and they do not want such information re-appearing in their competitors' offices.

-- How often will threat assessments be issued? This is currently undetermined. Our contacts opined that they should be issued regularly, even if unchanged, in order to remind users of their existence.

-- How widely will threat assessments be disseminated? A provincial government security official (who is a former RCMP officer) said it was a "major achievement" to persuade the RCMP to allow even unclassified versions of threat assessments to be shared with industry security officials (rather than only government agencies).

-- Who bears responsibility for formally declaring states of alert? This raises real issues of legal liability. According to our contacts in the Alberta government, the Solicitor General of Alberta (the senior provincial law enforcement officer) currently holds this responsibility (despite having limited access to intelligence information) and no office in the GOC will make a commitment to this function.

RELATIONSHIPS WITH USG

¶18. (SBU) Among our contacts, mentions of dealings with the USG on safety/security matters were strongly positive. The U.S. National Transportation Safety Board (NTSB) and Department of Transportation (DOT) investigate pipeline accidents which occur within the U.S., where both Enbridge and TransCanada have many facilities. In mid-2002 a rupture in Minnesota led to NTSB investigators paying an extended visit to Enbridge corporate headquarters in Edmonton. The report is still pending, but according to Enbridge the firm was commended for their quick response to the incident.

¶19. (SBU) Industry security officials say they receive regular notices from the FBI's National Infrastructure

Protection Center. One industry association leader told us his organization has a "very valuable relationship with the FBI" and that "we get better information from the FBI than from the RCMP." Our contacts also said they receive useful security-related information from the U.S. Department of Energy's Office of Energy Assurance and also from the American Petroleum Institute.

COMMENT

¶20. (SBU) The federal Government of Canada's Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) is relatively new and is still establishing itself in many areas of its mandate. While Mission staff are developing our relationship with and understanding of OCIPEP, we see great value in continuing to foster close cooperation with Provincial government authorities and private sector entities, such as the major pipeline and energy firms, who are now and will likely remain the first responders in an emergency.

CELLUCCI